REDACTED DOCUMENT

Docket # 25

Date Filed: 7/19/13

EL/GSG/2009R00080

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Jerome B. Simandle
	:	
v.	:	Criminal No. 09-626 (JBS) (S-2)
	:	
VLADIMIR DRINKMAN,	:	18 U.S.C. §§ 371, 1030, 1343, 1349, and 2
a/k/a	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
	:	
ALEKSANDR KALININ,	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
	:	
ROMAN KOTOV,	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
	:	
MIKHAIL RYTIKOV,	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
	:	
DMITRIY SMILIANETS,	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	
a/k/a	:	

SECOND SUPERSEDING INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

COUNT ONE
(Computer Hacking Conspiracy)

1. At various times relevant to this Second Superseding Indictment:

The Defendants

a. Defendant VLADIMIR DRINKMAN, a/k/a ' a/k/a a/k/a a/k/a ("DRINKMAN"), resided in or near Syktyvkar, Russia, and Moscow, Russia. As set forth more fully below, DRINKMAN was a sophisticated hacker, who specialized in penetrating and gaining access to the computer networks of multinational corporations, financial institutions and payment processors; harvesting data, including, among other things, credit card, debit card, and other customer account information, from within the compromised networks; and exfiltrating that data out of the compromised networks.

b. Defendant ALEKSANDR KALININ, a/k/a a/k/a a/k/a a/k/a a/k/a a/k/a ("KALININ"), resided in or near St. Petersburg, Russia. As set forth more fully below, KALININ was a sophisticated hacker, who specialized in penetrating and gaining access to the computer networks of multinational corporations, financial institutions and payment processors. After gaining access to such networks, KALININ and his co-conspirators stole data, including, among other things, credit card, debit card, and other customer account information, from the compromised networks.

c. Defendant ROMAN KOTOV, a/k/a a/k/a a/k/a ("KOTOV"), resided in or near Moscow, Russia. KOTOV specialized in harvesting data from within the computer networks that DRINKMAN and KALININ had penetrated, and exfiltrating that data.

d. Defendant MIKHAIL RYTIKOV, a/k/a a/k/a a/k/a a/k/a a/k/a a/k/a ("RYTIKOV"), resided in or near Odessa, Ukraine. As set forth more fully below, RYTIKOV provided anonymous web-hosting services to DRINKMAN, KALININ, KOTOV, and others, that they used to both hack into the computer networks of a number of victim companies, and exfiltrate (that is, covertly remove) data from the networks of those victims.

e. DMITRIY SMILIANETS, a/k/a a/k/a a/k/a a/k/a a/k/a a/k/a ("SMILIANETS"), resided in or near Moscow, Russia. As set forth more fully below, SMILIANETS was responsible for selling the information that DRINKMAN, KALININ, KOTOV, and others obtained through their hacking activities, and for disbursing the proceeds from the sale of that information to DRINKMAN, KALININ, KOTOV, and others.

Co-conspirators

f. Albert Gonzalez, a/k/a "segvec," a/k/a "soupnazi," a/k/a "j4guar17" ("Gonzalez"), a co-conspirator who is not charged as a defendant herein, resided in or near Miami, Florida.

g. Damon Patrick Toey ("Toey"), a co-conspirator who is not charged as a defendant herein, resided in or near Virginia Beach, Virginia, and in or near Miami, Florida.

h. Vladislav Anatolievich Horohorin ("Horohorin"), a/k/a "BadB," resided in or near Moscow, Russia.

i. Co-conspirator-1 ("CC#1"), a co-conspirator who is not charged as a defendant herein, resided in or near Kiev, Ukraine.

Overview of the Hacking Conspiracy

j. From at least as early as August 2005 through at least July 2012, defendants DRINKMAN, KALININ, KOTOV, RYTIKOV, and SMILIANETS (collectively the "Defendants"), together with their co-conspirators, operated a prolific hacking organization that was responsible for several of the largest known data breaches. Among other exploits during that period, the Defendants and their co-conspirators penetrated the secure computer networks of several of the largest payment processing companies, retailers, and financial institutions in the world, and stole the personal identifying information of others, such as user names and passwords ("Log-In Credentials"), means of identification ("Personal Data"), credit and debit card numbers ("Card Numbers"), and corresponding personal identification information of cardholders (collectively the "Stolen Data").

k. Conservatively, the Defendants and their co-conspirators unlawfully acquired over 160 million Card Numbers through their hacking activities. After acquiring this information, which they referred to as "dumps" – hacker shorthand for Card Numbers and associated data, the Defendants and their co-conspirators sold the dumps to "dumps resellers" around the world, who, in turn, sold them either through on-line forums or directly to individuals and organizations ("cashers"). Ultimately, the cashers encoded each dump onto the magnetic strip of a blank plastic card and cashed out the value of the dump by either withdrawing money from ATMs (in the case of a debit card dump), or incurring charges and purchasing goods (in the case of a credit card dump).

l. As a result of this conduct, financial institutions, credit card companies, and consumers suffered hundreds of millions in losses, including losses in excess of $300 million

by just three of the Corporate Victims, and immeasurable losses to the identity theft victims due to the costs associated with stolen identities and fraudulent charges.

Selected Methods of Hacking Utilized by Defendants

m. Structured Query Language ("SQL") was a computer programming language designed to retrieve and manage data in computer databases.

n. "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet.

o. "SQL Injection Strings" were a series of instructions to computers used by hackers in furtherance of SQL Injection Attacks.

p. "Malware" was malicious computer software programmed to, among other things, gain unauthorized access to computers; to identify, store, and export information from hacked computers; and to evade detection of intrusions by anti-virus programs and other security features running on those computers.

q. "Tunneling" was a method employed to create a connection between a hacked computer and an attacking computer to facilitate the transmission of, among other things, commands from the attacking computer to the hacked computer, and data from the hacked computer to the attacking computer.

The Corporate Victims of Computer Hacking

2. At various times relevant to this Second Superseding Indictment:

a. NASDAQ was the largest United States electronic stock market, and the primary market for trading in the stocks of approximately 3,200 public companies. NASDAQ offered its customers access to on-line accounts over the Internet, and its computer network was

located in, among other places, Middlesex County, New Jersey. Beginning in or about May 2007, NASDAQ was the victim of a SQL Injection Attack that resulted in the placement of malware on its network, and the theft of Log-in Credentials.

b. 7-Eleven, Inc. ("7-Eleven") was headquartered in Dallas, Texas, and was the corporate parent of a convenience store chain by the same name. 7-Eleven processed credit and debit card transactions through its computer networks. Beginning in or about August 2007, 7-Eleven was the victim of a SQL Injection Attack that resulted in malware being placed on its network and the theft of an undetermined number of Card Numbers.

c. Carrefour S.A. ("Carrefour") was a French multinational retailer headquartered in Greater Paris, France, and was one of the largest retailers in the world in terms of revenue and profit. Beginning as early as October 2007, Carrefour's computer networks were breached and approximately 2 million credit Card Numbers were subsequently exfiltrated.

d. JCPenney, Inc. ("JCP") was a major national retailer with its headquarters in Plano, Texas. JCP processed credit card payments for its retail stores through its computer network. Beginning on or about October 23, 2007, JCP was the victim of a SQL Injection Attack that resulted in the placement of malware on its network.

e. Hannaford Brothers Co. ("Hannaford") was a regional supermarket chain with stores located in Maine, New Hampshire, Vermont, Massachusetts, and New York that processed credit and debit card transactions through its computer network. In or about early November 2007, a related company of Hannaford was the victim of a SQL Injection Attack that resulted in the later placement of malware on Hannaford's network, the theft of approximately 4.2 million Card Numbers.

f. Heartland Payment Systems, Inc. ("Heartland"), which was located in or near Princeton, New Jersey, and Plano, Texas, among other places, was one of the world's largest credit and debit card payment processing companies. Heartland processed millions of credit and debit transactions daily. Beginning on or about December 26, 2007, Heartland was the victim of a SQL Injection Attack on its corporate computer network that resulted in malware being placed on its payment processing system and the theft of more than approximately 130 million Card Numbers, and losses of approximately $200 million.

g. Wet Seal, Inc. ("Wet Seal") was a major national retailer with its headquarters in Foothill Ranch, California. Wet Seal processed credit and debit card payments for its retail stores through its computer network. In or about January 2008, Wet Seal was the victim of a SQL Injection Attack that resulted in the placement of malware on its network.

h. Commidea Ltd. ("Commidea") was a European provider of electronic payment and transaction processing solutions for retailers, with its headquarters in the United Kingdom. From at least as early as March 2008 through in or about November 2008, malware used in other known network intrusions existed on Commidea's computer networks, and was communicating with known hacking platforms. In or about 2008, approximately 30 million Card Numbers were exfiltrated from Commidea's computer networks.

i. Dexia Bank Belgium ("Dexia") was a consumer bank located in Belgium. Between in or about February 2008 and in or about February 2009, Dexia was the victim of SQL Injection Attacks that resulted in the placement of malware on its network and the theft of Card Numbers that resulted in approximately $1.7 million in loss.

j. JetBlue Airways ("JetBlue") was an airline with its headquarters in Long Island City, New York. Between in or about January 2008 and in or about February 2011, JetBlue suffered an unauthorized intrusion resulting in the placement of malware on portions of its computer network that stored Personal Data of its employees.

k. Dow Jones, Inc. ("Dow Jones") published news, business, and financial information worldwide in newspapers, on television and radio, over news wires, and on the Internet. Dow Jones's computer infrastructure was based largely in New Jersey, as well as in Minnesota, New York and elsewhere. In or before 2009, Dow Jones was the victim of unauthorized access to its computer network resulting in the placement of malware on its network and the theft of approximately 10,000 sets of Log-In Credentials.

l. "Bank A" was one of the leading domestic banks in the United Arab Emirates, and was headquartered in Abu Dhabi. Between in or about December 2010 and in or about March 2011, malware was placed on Bank A's computer networks, and was used to facilitate the theft of Card Numbers.

m. Euronet was a global provider of electronic payment and transaction processing solutions for financial institutions, retailers, service providers and individual consumers, with its headquarters in Leawood, Kansas. Between in or about July 2010 and in or about October 2011, Euronet was the victim of SQL Injection Attacks that resulted in the placement of malware on its network and the theft of approximately 2 million Card Numbers.

n. Visa, Inc. ("Visa") was a global payments technology company that owned and managed the "Visa" brand. Visa did not directly issue credit or debit cards, extend credit, or set rates and fees for consumers. Rather, it provided processing services to its financial

institution clients through "VisaNet," a centralized and modular payments network. Visa Jordan Card Services ("Visa Jordan") was a Visa licensee, and Jordan's premier payment card processor. Between in or about February 2011 and in or about March 2011, Visa Jordan was the victim of SQL Injection Attacks that resulted in the placement of malware on its network, and the theft of approximately 800,000 Card Numbers.

o. Global Payment Systems ("Global Payment") was one of the world's largest electronic transaction processing companies, with its headquarters in Atlanta, Georgia. Between in or about January 2011 and in or about March 2012, Global Payment was the victim of SQL Injection Attacks on its computer network that resulted in malware being placed on its payment processing system and the theft of more than 950,000 Card Numbers, and losses of approximately $92.7 million.

p. Discover Financial Services, Inc. was a financial services company, which, among other things, issued the Discover Card credit card, and since in or about April 2008 has owned the Diners Club International ("Diners") charge card network. Diners provided a variety of payment solutions to its customers and managed the Diners brand, which was licensed to a number of international franchisees, including Diners Singapore. Beginning on or about June 23, 2011, Diners Singapore was the victim of an SQL Injection Attack that resulted in malware being placed on its network and the theft of Card Numbers; the intrusion exposed over 500,000 Diners credit cards and resulted in losses of approximately $312,000.

q. Ingenicard US, Inc. ("Ingenicard") was a provider of international electronic cash cards headquartered in Miami, Florida, and operated one of the largest cash exchange platforms in the world. From in or about March 2012 through in or about December

2012, Ingenicard was the victim of SQL Injection Attacks that resulted in malware being placed on its network and the theft of Card Numbers, which were later used to withdraw over $9 million within twenty-four hours.

r. NASDAQ, 7-Eleven, Carrefour, JCP, Hannaford, Heartland, Wet Seal, Commidea, Dexia, JetBlue, Dow Jones, Bank A, Euronet, Visa Jordan, Global Payment, Diners, and Ingenicard are collectively referred to herein as the "Corporate Victims."

THE CONSPIRACY

3. Between in or about August 2005 and in or about July 2012, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a "
a/k/a '

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a

ROMAN KOTOV,
a/k/a
a/k/a
a/k/a

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a

and

DMITRIY SMILIANETS,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a

did knowingly and intentionally conspire and agree with each other, Gonzalez, Toey, CC #1, and others to commit offenses against the United States, namely:

a. by means of interstate communications, intentionally accessing computers in interstate commerce without authorization, and exceeding authorized access, and thereby obtaining information from those computers, namely Log-In Credentials, Personal Data, and Card Numbers, for the purpose of commercial advantage and private financial gain, contrary to Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i); and

b. knowingly and with intent to defraud accessing computers in interstate commerce without authorization and exceeding authorized access to such computers, and by means of such conduct furthering the intended fraud and obtaining anything of value, namely Log-In Credentials, Personal Data, and Card Numbers, contrary to Title 18, United States Code, Section 1030(a)(4).

OBJECT OF THE CONSPIRACY

4. It was the object of the conspiracy for DRINKMAN, KALININ, KOTOV, RYTIKOV, SMILIANETS, Gonzalez, Toey, CC #1, and others to hack into the Corporate Victims' computer networks in order to steal and then sell Log-In Credentials, Personal Data, and Card Numbers, or to otherwise profit from their unauthorized access.

MANNER AND MEANS OF THE CONSPIRACY

5. The manner and means by which DRINKMAN, KALININ, KOTOV, RYTIKOV, SMILIANETS, Gonzalez, Toey, CC #1, and others, sought to accomplish the conspiracy included, among other things, the following:

Scouting Potential Victims

a. It was part of the conspiracy that DRINKMAN, KALININ, KOTOV, Gonzalez, and Toey would identify corporate victims by researching websites and other publications to find corporations that engaged in financial transactions.

b. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, Gonzalez, and Toey would probe potential vulnerabilities in the websites of the corporations they discovered in their research to identify potential corporate victims.

c. It was further part of the conspiracy that between in or about 2007 and in or about 2008, Gonzalez and Toey would travel to retail stores of potential corporate victims in order to first identify the payment processing systems that the would-be victims used at their point of sale terminals (e.g., "checkout" computers) and then to understand the potential vulnerabilities of those systems.

Launching the Attacks – The Hacking Platforms

d. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, SMILIANETS, Gonzalez, and others would lease, control, and use Internet-connected computers in New Jersey ("the Net Access Server"), Pennsylvania ("the BurstNet Server"), California ("the ESTHOST Server"), Illinois ("the Giganet Server"), Latvia ("the Latvian Server"), the Netherlands ("the Leaseweb Server"), Ukraine, the Bahamas, Panama, Germany

and elsewhere (collectively, "the Hacking Platforms") to (1) store malware; (2) stage attacks on the Corporate Victims' networks; and (3) receive stolen Log-In Credentials, Personal Data, and Card Numbers from these networks.

e. It was further part of the conspiracy that RYTIKOV would lease some of the Hacking Platforms to KALININ, SMILIANETS, and others for use in attacking the Corporate Victims' networks.

f. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, Gonzalez, Toey, and others would provide each other and others with SQL Injection Strings and malware that could be used to gain unauthorized access to the Corporate Victims' networks and to locate, store, and transmit Log-In Credentials, Personal Data, and Card Numbers from those networks.

g. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, Gonzalez, Toey, and others would hack into the Corporate Victims' networks using various techniques, including, among others, SQL Injection Attacks, to steal, among other things, Log-In Credentials, Personal Data, and Card Numbers.

Executing the Attacks - The Malware

h. It was further part of the conspiracy that once they hacked into the Corporate Victims' computer networks, DRINKMAN, KALININ, KOTOV, Gonzalez, and others would place unique malware on the Corporate Victims' networks that would enable them to access these networks at a later date ("Back Doors").

i. It was further part of the conspiracy that once they hacked into the Corporate Victims' networks, DRINKMAN, KALININ, KOTOV, Gonzalez, and others would

conduct network reconnaissance for the purpose of finding and stealing Log-In Credentials, Personal Data, Card Numbers, and other valuable information within the Corporate Victims' networks.

j. It was further part of the conspiracy that once DRINKMAN, KALININ, KOTOV, Gonzalez, and others hacked into the Corporate Victims' networks, they would install "sniffer" programs that would capture Card Numbers, and other information on a real-time basis as the information moved through the Corporate Victims' credit and debit card processing networks, and then periodically transmit that information to the co-conspirators.

k. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, Gonzalez, Toey, and others would communicate via instant messaging services while their unauthorized access was taking place in order to advise each other as to how to navigate the Corporate Victims' networks and how to locate Log-In Credentials, Personal Data, Card Numbers, and other valuable information.

l. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, Gonzalez, and others would use unique malware to transmit the Log-In Credentials, Personal Data, Card Numbers, and other valuable information to a Hacking Platform.

Concealing the Attacks

m. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, SMILIANETS, Gonzalez, Toey, and others would conceal their efforts to hack into the Corporate Victims' networks by, among other things, leasing the Hacking Platforms under false names.

n. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, Gonzalez, Toey, and others would conceal their attacks by disguising, through the use of "proxies," the Internet Protocol addresses from which their attacks originated.

Bullet-proof Hosting

o. It was further part of the conspiracy that RYTIKOV offered "bullet-proof hosting" services to his co-conspirators (*i.e.*, leasing servers from which law enforcement supposedly could not gain access or obtain information). "Bullet-proof hosting" services included frequently changing the locations of Hacking Platforms, erasing the contents of Hacking Platforms on short notice, accepting false credentials to register and lease Hacking Platforms, and discouraging Internet Service Providers from deactivating Hacking Platforms suspected of illegal activity.

Advanced Techniques

p. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, SMILIANETS, Gonzalez, Toey, and others would conceal their efforts by storing data related to their attacks on multiple Hacking Platforms, disabling programs that logged inbound and outbound traffic over the Hacking Platforms, and frequently moving between different Hacking Platforms.

q. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, Gonzalez, and Toey would conceal their efforts to hack into the Corporate Victims' networks by, among other things, programming malware to be placed on the Corporate Victims' computer networks to evade detection by anti-virus software.

Communications

r. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, SMILIANETS, Gonzalez, Toey, and others would conceal their efforts by communicating over the Internet using more than one messaging screen name. After becoming aware that law enforcement tracked certain communications using known messaging services, the co-conspirators established private and encrypted communications channels to avoid detection. Fearing that even these encrypted communication channels could be monitored, several of the co-conspirators ultimately attempted to conduct their communications in person.

Profiting from the Attacks

s. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, and others would provide SMILIANETS with dumps to sell.

t. It was further part of the conspiracy that SMILIANETS would sell the dumps to dumps resellers, who, in turn, sold them to individuals that encoded them onto the magnetic strips of blank plastic cards, which they and others used to make unauthorized ATM withdrawals and to incur unauthorized credit card charges.

u. It was further part of the conspiracy that SMILIANETS would set the prices for the dumps that he sold, and would charge approximately $10 for each stolen American credit card number and associated data; approximately $50 for each European credit card number and associated data; and approximately $15 for each Canadian credit card number and associated data. In addition, SMILIANETS offered discounted pricing to bulk and repeat customers.

v. It was further part of the conspiracy that SMILIANETS would direct that payments for dumps that he sold be sent through Western Union, MoneyGram, or international

wire transfer to individuals and accounts controlled by CC#1, a money exchanger based in Kiev, Ukraine.

w. It was further part of the conspiracy that CC#1, after deducting a fee, would forward money he received on SMILIANETS's behalf to SMILIANETS by, among other things, depositing it directly into WebMoney[1] accounts that SMILIANETS controlled, and sending cash from Ukraine to Russia through couriers recruited by CC#1, SMILIANETS, and others.

OVERT ACTS

6. In furtherance of the conspiracy, and to effect its unlawful objects, the co-conspirators committed and caused to be committed the following criminal acts, among others, in the District of New Jersey and elsewhere:

NASDAQ and JetBlue

7. On or about May 19, 2007, KALININ identified a security vulnerability at a NASDAQ web page that enabled NASDAQ's customers to obtain on-line password reminders ("the Remind Me Site").

8. On or before May 24, 2007, KALININ used a SQL Injection Attack to obtain encrypted Log-In Credentials from NASDAQ's Remind Me Site and sent it via instant message to Gonzalez.

9. On or about May 24, 2007, KALININ sent Gonzalez a SQL Injection String that Gonzalez could use to access NASDAQ's computer network without authorization.

---

[1] WebMoney was an electronic money and online payment system based and operated from Russia.

10. On or about August 12, 2007, after KALININ accessed NASDAQ's computer network, KALININ sent Gonzalez an instant message stating that the network was about "30 SQL servers, and we can run whatever on them, already cracked admin PWS but the network not viewable yet." KALININ further commented that "those dbs are hell big and I think most of info is trading histories."

11. On or about January 9, 2008, in response to an offer from Gonzalez to help attack NASDAQ, KALININ told Gonzalez via instant message that "NASDAQ is owned."

12. On or before January 9, 2008, KALININ obtained administrative access – that is, access sufficient to permit him to perform network or systems administrator functions – to NASDAQ's computer network, and noted to Gonzalez via instant message that he had maintained that access for a long time.

13. On or about March 18, 2008, KALININ wrote to Gonzalez via instant message that DRINKMAN had lost "back door" access to NASDAQ, that KALININ had reacquired it, and that KALININ would not lose it again.

14. Between on or about August 28, 2008 and in or about March 2009, KALININ rented a Hacking Platform in the Bahamas ("the Bahamas Server") from RYTIKOV.

15. On or about November 26, 2008, KALININ caused the insertion of an unauthorized file named "hcx.txt" on the NASDAQ network. "hcx.txt" was pre-programmed to assist in communications with the Bahamas Server that KALININ rented from RYTIKOV.

16. On or about December 10, 2008, KALININ caused the insertion of hcx.txt on the JetBlue network. "hcx.txt" was pre-programed to assist in communications with the Bahamas Server that KALININ rented from RYTIKOV.

17. In or about October 2009, a co-conspirator caused a NASDAQ computer to attempt to communicate with the Bahamas Server that KALININ rented from RYTIKOV.

Carrefour

18. On or about October 29, 2007, during an instant messaging chat, Gonzalez and KALININ discussed a vulnerability in Carrefour's network:

KALININ: I have some big europe retailer...

Gonzalez: carrefour?

KALININ: ya

Gonzalez: they're BIG

KALININ: I just picked up a top100 retailers

KALININ: saw them on 2nd place

KALININ: their networks seems to be connected, cuz I saw france etc hacking spain one

19. On or about October 30, 2007, KALININ informed Gonzalez that he and DRINKMAN had established access into Carrefour's computer networks:

KALININ: yo

Gonzalez: whats up?

KALININ: just woke up, got a shell[2] from carrefour with [DRINKMAN] finally

KALININ: about you?

Gonzalez: [DRINKMAN] is online?

---

[2] A "shell" was software that provided an user with access to a computer's operating system, and in this case was used by KALININ and his co-conspirators to remotely access a victim computer's network.

KALININ: yep

Gonzalez: is [DRINKMAN] owning carrefour?

KALININ: yep

20. Between in or about 2007 and in or about 2008, DRINKMAN, KALININ and KOTOV accessed Carrefour's network and exfiltrated approximately 2 million Card Numbers from Carrefour's computer networks.

21. Following the intrusion described above, SMILIANETS sold dumps obtained from Carrefour's computer networks.

Heartland and JCP

22. On or about November 6, 2007, Gonzalez transferred a computer file named "sqlz.txt" that contained information stolen from JCP's computer network to a Hacking Platform in Ukraine ("the Ukraine Server").

23. On or about November 6, 2007, Gonzalez transferred a computer file to the Ukraine Server named "injector.exe" that matched malware placed on both Heartland and JCP's servers during the hacks of those companies.

24. On or about December 26, 2007, DRINKMAN and KALININ accessed Heartland's computer network by means of a SQL Injection Attack from the Leaseweb Server and using the ESTHOST Server.

25. Following the intrusion described above, SMILIANETS sold dumps obtained from Heartland's computer networks. For example, between in or about February 2008 and in or about March 2008, SMILIANETS sent Horohorin, a known and prolific dumps reseller, instant

messages providing Card Numbers obtained by DRINKMAN and KALININ from the Heartland hack.

Wet Seal

26. During an instant messaging chat on or about December 4, 2007, Gonzalez and KALININ discussed potential vulnerabilities in Wet Seal's network:

KALININ: yo

Gonzalez: whats up?

KALININ: I forgot again what I was going to tell heh

Gonzalez: I asked [DRINKMAN] for some help finding sql'ing in wetseal.com I think I found one in http://web.wetseal.com[...].

KALININ: vulnerable

Gonzalez: how did you check?

27. In or about January 2008, over an instant messaging service, Gonzalez sent Toey a SQL Injection String that was used to penetrate Wet Seal's computer network (the "Wet Seal SQL String"). The Wet Seal SQL String was programmed to direct data to Hacking Platforms, including the ESTHOST Server and the Ukraine Server.

28. During an instant messaging chat on or about April 18, 2008, Gonzalez and KALININ discussed ways in which to explore Wet Seal's network:

Gonzalez: wetseal is a big retail place in usa

KALININ: ok

* * * *

Gonzalez: how do I get a shell into wetseal so I can look around too?

KALININ: [REDACTED COMMAND]

KALININ: I quit

KALININ: [REDACTED PORT NUMBER]

Gonzalez: you're using [REDACTED PORT NUMBER] though :)

Gonzalez: ahh ok

Gonzalez: how did you get on the web servers?

KALININ: [REDACTED COMMAND]

KALININ: this one is web

* * * *

Gonzalez: btw, can you ask [DRINKMAN] for his universal hooker/logger[3] for wetseal?

KALININ: I cant get him online last days

29. On or about April 22, 2008, Gonzalez modified a file on the Ukraine Server that contained computer log data stolen from Wet Seal's computer network.

30. Between in or after March 2007 and in or about May 2008, Gonzalez participated in a discussion over an instant messaging service in which one of the participants stated "core still hasn't downloaded that Wet Seal sh-t."

Commidea

31. Before in or about March 2008, DRINKMAN and KOTOV caused the insertion of a file named "msdll.exe" on Commidea's computer network, which allowed outside users to run programs on Commidea's network.

---

[3] "Hookers" and "loggers" were types of malware used by hackers to intercept and log network activity and data.

32. In or about 2008, DRINKMAN and KOTOV exfiltrated approximately 30 million Card Numbers.

33. Following the intrusion described above, SMILIANETS sold dumps obtained from Commidea's networks, including sales between February 2008 and November 2008 to Horohorin.

Hannaford

34. Between in or after March 2007 and in or about May 2008, Gonzalez participated in a discussion over an instant messaging service in which one of the participants stated "planning my second phase against Hannaford."

35. Between in or after December 2007 and in or about May 2008, Toey participated in a discussion over an instant messaging service in which one of the participants stated "that's how [DRINKMAN] hacked Hannaford."

36. During an instant messaging chat on or about March 18, 2008, Gonzalez forwarded KALININ a link to an article discussing the intrusion into Hannaford's networks and discussed the breach with him.

37. Thereafter, during instant messaging chats between on or about March 18, 2008 and April 23, 2008, Gonzalez and KALININ once again discussed the Hannaford breach:

KALININ: haha they had hannaford issue on tv news?

Gonzalez: not here

Gonzalez: I have triggers set on google news for things like "data breach" "credit card fraud" "debit card fraud" "atm fraud" "hackers"

Gonzalez: I get emailed news articles immediately when they come out, you should do the same, its how I find out when my hacks are found :)

* * * *

Gonzalez: hannaford lasted 3 month of sales before it was on news, im trying to figure out how much time its gonig [*sic*] to be alive for

* * * *

Gonzalez: hannaford will spend millions to upgrade their security!! lol

KALININ: haha

KALININ: they would better pay us to not hack them again

38. Following the intrusion described above, SMILIANETS sold dumps obtained from Hannaford's computer networks.

Dexia

39. Between in or about May 2008 and in or about August 2008, KALININ leased a Hacking Platform from RYTIKOV located in Panama ("the Panama Server").

40. Between in or about February 2008 and in or about August 2008, a co-conspirator caused the insertion of a file named "L.exe" on Dexia's computer network. "L.exe," which allowed outside users to run programs on Dexia's network, was the same file used in the attacks on Heartland and JCP. Gonzalez also hosted the same file on the Ukraine Server.

41. On or about August 4, 2008, during the time that KALININ leased the Panama Server from RYTIKOV, KALININ caused Dexia's network to establish a file transfer connection with the Panama Server.

42. On or about August 27 and August 28, 2008, KALININ instructed RYTIKOV via instant message to reinstall the operating system on the Panama Server, effectively erasing it, and to give this server to a different customer.

Dow Jones and the Odessa Server

43. On or about August 8, 2008, KALININ asked RYTIKOV through instant message to custom-build him a Hacking Platform.

44. Between on or about August 8, 2008 and on or about August 11, 2008, RYTIKOV built a Hacking Platform for KALININ that was located in Odessa, Ukraine ("the Odessa Server").

45. On or about August 11, 2008, RYTIKOV gave access to the Odessa Server to KALININ and assigned it to a particular Internet Protocol address.

46. Later that day, KALININ complained to RYTIKOV that the network speed to the Odessa Server was not fast enough for KALININ because KALININ needed to be able to download approximately 32 gigabytes of information at one time.

47. On or about August 18, 2008, KALININ used the Odessa Server to store "rainbow tables," which were lists of possible passwords made for use with password-cracking software. The lists of possible passwords in rainbow tables were approximately 34 gigabytes in size.

48. On or about December 13, 2008, in connection with providing "bullet-proof hosting" services, RYTIKOV's data center assigned the Odessa Server a new Internet Protocol address and advised KALININ via instant message of the new Internet Protocol address for the Odessa Server.

49. In or about February 2009, in connection with providing "bullet-proof hosting" services, RYTIKOV assigned the Odessa Server a new Internet Protocol address and advised KALININ via instant message of that new Internet Protocol address for the Odessa Server.

50. On or about May 18, 2009, KALININ attempted to connect to the Odessa Server and told RYTIKOV via instant message that he was having trouble.

51. Between in or about August 2008 and on or about June 24, 2009, KALININ used the Odessa Server to store and later delete approximately 30,000 sets of Log-In Credentials (mainly user names and encrypted passwords) belonging to Dow Jones employees and Dow Jones user accounts.

52. Between on or about August 28, 2008 and on or about June 24, 2009, KALININ used the Odessa Server to open a file transfer connection with the Bahamas Server used in the attack on NASDAQ and JetBlue.

Euronet

53. Between in or about July 2010 and in or about December 2011, a co-conspirator caused the insertion of a file named "medll.exe" on Euronet's computer network, which allowed outside users to run programs on Euronet's network from the German Leaseweb and Hetzner Online Servers. "medll.exe" used the same unique encryption key as the malware used in the Dow Jones and JCP intrusions described above, among others.

54. Between in or about February 2010 and in or about April 2011, KALININ accessed the German Leaseweb and Hetzner Online Servers on multiple occasions, and on a number of occasions downloaded executable files from the German Leaseweb or Hetzner Online Servers, including malware.

Global Payment Systems

55. In or about January 2011, a co-conspirator caused the insertion of a file named "medll.exe" on Global Payment's computer network, which allowed outside users to run programs on Euronet's network from the German Leaseweb and Hetzner Online Servers. "medll.exe" used the same unique encryption key as the malware used in the Dow Jones, JCP, and Euronet intrusions described above, among others.

56. In or about 2011, the German Leaseweb or Hetzner Online Servers were used to access Internet Protocol addresses associated with Global Payments.

Bank A

57. In or about 2010, KALININ gained access to the computer networks of Bank A.

58. In or about 2010, DRINKMAN asked SMILIANETS to open an account at Bank A to assist DRINKMAN in learning how Bank A's computer networks operated.

59. From in or about 2010 through in or about 2012, DRINKMAN, KALININ and KOTOV used the same Hetzner Online Server that was used in the Euronet and Global Payments intrusions to facilitate access into Bank A's networks.

Visa Jordan

60. In or about 2009, KALININ discovered a vulnerability in Visa Jordan's network, and gained access to it by means of a SQL Injection Attack.

61. On or about February 27, 2011, KALININ and others accessed Visa Jordan's network from the IP address XX.XXX.80.94, which was also used to access a Hacking Platform used in the Euronet intrusion in or around the same time period.

62. On or about March 3, 2011, KALININ and others accessed Visa Jordan's network from the IP address XX.XXX.223.210, which was also used to access a Hacking Platform used in the Euronet intrusion in or around the same time period.

63. On or about March 29, 2011, KALININ and others accessed Visa Jordan's network from the IP address XX.XX.24.29, issued commands, and created a remote access tunnel to IP address XX.XXX.223.136, which was used to access Global Payment's network during the same period.

64. In or about 2011, KALININ, DRINKMAN and others exfiltrated approximately 800,000 Card Numbers from Visa Jordan's computer networks.

65. Following the intrusion described above, SMILIANETS sold dumps obtained from Visa Jordan's networks.

Diners Singapore

66. Between in or about June 2011 and May 2012, KALININ discovered a vulnerability in Diners Singapore's network, and gained access to it by means of a SQL Injection Attack.

67. In or about June 2011, KALININ and DRINKMAN loaded malware named "mint.exe" onto Diners Singapore's computer networks to establish a remote connection to a server they controlled. The same file was used in the attack on Global Payment.

68. In or about June 2011, KALININ and DRINKMAN loaded malware named "tt.vbs" onto Diners Singapore's computer networks to facilitate the downloading of files from the networks. A similar file was used in the attack on Global Payment.

69. In or about June 2011, KALININ and DRINKMAN downloaded malware onto Diners Singapore's computer networks from a compromised Swiss server used to host malware, which was also used to download some of the same malware onto Global Payment's and Ingenicard's networks.

70. In or about December 2011, KALININ and DRINKMAN established an encrypted tunnel from Diners Singapore's computer networks to servers they controlled in order to facilitate the exfiltration of dumps from Diners Singapore computer networks.

Ingenicard

71. Beginning on or about March 21, 2012, DRINKMAN gained access to Ingenicard's computer networks.

72. On or about March 21, 2012, DRINKMAN downloaded three pieces of malware – "gsc.exe," "gsc2.exe," and "sl.exe" – onto an Ingenicard computer server from the same compromised Swiss server discussed in paragraph 69 above that was also used to download some of the same malware onto Global Payment's networks.

73. After gaining access to Ingenicard's networks, DRINKMAN manipulated Ingenicard's systems to permit unlimited withdrawals from Ingenicard customer accounts. Thereafter, DRINKMAN exfiltrated approximately 23 Card Numbers from Ingenicard's computer networks, which were later used to withdraw over $9 million within a twenty-four hour period.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO
(Conspiracy to Commit Wire Fraud)

1. The allegations contained in paragraphs 1, 2, and 6 through 73 of Count One of the Second Superseding Indictment are realleged and incorporated as if set forth herein.

2. Between in or about October 2006 and in or about July 2012, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a "
a/k/a '

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a

ROMAN KOTOV,
a/k/a
a/k/a
a/k/a

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a '
a/k/a
a/k/a

and

DMITRIY SMILIANETS,
a/k/a
a/k/a '
a/k/a "
a/k/a
a/k/a

a/k/a

did knowingly and intentionally conspire and agree with each other, Gonzalez, Toey, CC#1, and others to devise a scheme and artifice to defraud the Corporate Victims, their customers, and the financial institutions that issued credit and debit cards to those customers, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing the scheme and artifice to defraud, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for DRINKMAN, KALININ, KOTOV, SMILIANETS, Gonzalez, Toey, CC#1, and others to profit from the sale and fraudulent use of Card Numbers stolen from the Corporate Victims' computer networks.

MANNER AND MEANS OF THE CONSPIRACY

4. It was part of the conspiracy that once the co-conspirators had obtained Card Numbers and other valuable data from the Corporate Victims' computer networks, DRINKMAN, KALININ, KOTOV, SMILIANETS, Gonzalez, Toey, CC#1, and others would cause the Card Numbers and associated data to be broken down into batches suitable for wholesale distribution over the Internet, for sale as dumps.

5. It was further part of the conspiracy that DRINKMAN, KALININ, KOTOV, SMILIANETS, Gonzalez, Toey, and others would sell the dumps using wire communications in interstate and foreign commerce and cause it to be available for resale.

6. It was further part of the conspiracy that those who purchased dumps would further distribute them throughout the United States and elsewhere using wire communications in interstate and foreign commerce, where they would be used to make unauthorized purchases at retail locations, to make unauthorized withdrawals from banks and financial institutions, and to further identity theft schemes.

All in violation of Title 18, United States Code, Section 1349.

COUNTS THREE THROUGH EIGHT
(Unauthorized Computer Access)

1. The allegations contained in paragraphs 1, 2, and 6 through 73 of Count One of the Second Superseding Indictment are realleged and incorporated as if set forth herein.

2. On or about the dates set forth below, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a "
a/k/a '

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a

ROMAN KOTOV,
a/k/a
a/k/a '
a/k/a

and

DMITRIY SMILIANETS,
a/k/a
a/k/a
a/k/a '
a/k/a '
a/k/a
a/k/a

by means of interstate communications, did intentionally access computers without authorization, and exceeded authorized access, namely the computer systems used in and affecting interstate and foreign commerce and communication owned by the Corporate Victims identified below,

and thereby obtained information from those computers, namely Log-In Credentials, Personal Data, and Card Numbers, for the purpose of commercial advantage and private financial gain:

Count	Approximate Date	Corporate Victim
3	August 2007	7-Eleven
4	October 23, 2007	JC Penney
5	December 26, 2007	Heartland
6	January 2008	Wet Seal
7	January 2008	JetBlue
8	2009	Dow Jones

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i).

COUNTS NINE THROUGH ELEVEN
(Wire Fraud)

1. The allegations contained in paragraphs 1, 2, and 6 through 73 of Count One of the Second Superseding Indictment are realleged and incorporated as if set forth herein.

2. On or about the dates set forth below, in Mercer and Middlesex Counties, in the District of New Jersey, and elsewhere, defendants

VLADIMIR DRINKMAN,
a/k/a
a/k/a "
a/k/a '

ALEKSANDR KALININ,
a/k/a "
a/k/a '
a/k/a '
a/k/a
a/k/a
a/k/a

ROMAN KOTOV,
a/k/a
a/k/a
a/k/a

and

DMITRIY SMILIANETS,
a/k/a
a/k/a '
a/k/a "
a/k/a

a/k/a
a/k/a

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud and to obtain money and property from the Corporate Victims identified below by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice, did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely, Log-In Credentials and Card Numbers.

Count	Approximate Date	Corporate Victim
9	August 2007	7-Eleven
10	December 26, 2007	Heartland
11	2009	Dow Jones

All in violation of Title 18, United States Code, Sections 1343 and Section 2.

A TRUE BILL

_____
FOREPERSON

Paul J. Fishman/rah
PAUL J. FISHMAN
United States Attorney

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

VLADIMIR DRINKMAN,
a/k/a
a/k/a
a/k/a

ALEKSANDR KALININ,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a

ROMAN KOTOV,
a/k/a
a/k/a
a/k/a

MIKHAIL RYTIKOV,
a/k/a
a/k/a
a/k/a
a/k/a
a/k/a

and DMITRIY SMILIANETS,
a/k
a/k/
a/k/
a/k/a
a/k/
a/k/a

INDICTMENT FOR
18 U.S.C. §§ 371, 1030, 1343, 1349, and 2

A True Bill,

Foreperson

PAUL J. FISHMAN
UNITED STATES ATTORNEY
NEWARK, NEW JERSEY

EREZ LIEBERMANN & GURBIR S. GREWAL
ASSISTANT U.S. ATTORNEYS
973-645-2874/2931

USA-48AD 8
(Ed. 1/97)